REMARKS

This is in response to the Office Action dated November 12, 2008. Applicant has amended the application as set forth above. In specific, claims 1-5 have been amended. All the features of the amended claims are fully supported by the originally filed application. Thus, the amendments do not add new matter to the application. Upon the entry of the amendments, claims 1-6 are pending in this application. Applicant respectfully requests the entry of the amendments and reconsideration of the application.

Claim Rejections under 35 U.S.C. §112, 1st and 2nd paragraphs

The Examiner rejected claims 1-6 under 35 U.S.C. §112, second paragraph. as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention, and claims 5 and 6 under 35 U.S.C. §112, first paragraph, because the specification, while being enabling for performing a function if the application module is authorized, does not reasonably provide enablement of performing a function if the application module is unauthorized.

In response, Applicant has amended Claims 1-5. Withdrawal of the objections is requested respectfully.

Claim Rejections under 35 U.S.C. §102

The Examiner rejected claims 1-6 under 35 U.S.C. §102(e) as being anticipated by Waldspurger et al. (USP 7,428,636). Applicant respectfully disagrees with the Examiner. However, in order to clarify the inventive points of the invention, Applicant has amended Claims 1-5.

Amended Claim 1 (*emphasis added*)

An access control system, comprising:

a Virtual Secure Disk (VSD) image file module occupying a certain space of a hard disk in a file form;

a VSD drive for processing security-sensitive files within the VSD image file module;

an encryption and decryption module for encrypting and decrypting data input, output, or input and output between the VSD image file module and the VSD drive:

a VSD file system module for allowing an operating system to recognize the VSD drive as a separate disk volume at a time of access to the security-sensitive files within the VSD image file module; and

an access control module for determining access by determining whether an access location is a disk drive or the VSD drive and an application module has been authorized to access a file, which is stored on the hard disk, to perform tasks in the application module,

wherein an authorized application module is configured to access the VSD drive for write and read operations, wherein the authorized application module is configured to access the disk drive for a read operation only, wherein an unauthorized application module is configured to access the disk drive for write and read operations, and wherein the unauthorized application module is not allowed to access the VSD drive.

Waldspurger Does Not Anticipate Claim 1

Claim 1 of the present invention comprises a VSD image file module, a VSD drive, an encryption and decryption module, a VSD file system module, and an access control module. The access to drives (a VSD drive and a disk drive) by application module is controlled, *such that an authorized application module can read and write to the VSD drive, but not write to the disk drive, and an unauthorized application module can read and write to the disk drive, but neither read nor write to the VSD drive.* Thereby, the VSD drive holds security-sensitive files only, which can be accessed by the authorized application module, and concurrently even the authorized application module can NOT write out to the disk drive (for regular, non-security-sensitive files), so as to protect the security-sensitive files just within the VSD drive. (See Figs. 1 and 2)

Whereas, Waldspurger discloses a selective encryption system and method for I/O operations. A disk can hold any type of data irrespective of "security-sensitive", but some of the data is encrypted and decrypted in writing and reading. Under this formatt, a data structure is marked to indicate which units are encrypted such that only those allocation units marked as encrypted are decrypted, so as to obtain a selective encryption and convenient automatic decryption using the data structure indicating which units are encrypted. (See Abstract. Fig. 3; col. 14, line 19 through col. 17, line 11).

In other words, Waldspurger does not discriminate the disk space for security-sensitive files and general files. A disk can hold any type of data, security-sensitive or not. As shown in Fig. 3, *the encrypted data (shown as D*) is written to the virtual disk 514 at the location specified by its corresponding block identifier B. If no encryption is to be performed, then D will be used directly instead of D*, since no encrypting will be necessary.* (See col. 10, lines 10-14).

Thus, there does NOT exist such scheme allowing a certain application module to read, write, or read-and-write to either of the VSD drive and the regular disk drive in Waldspurger's disclosure. Waldspurger just discloses selective encryption of some of the data, and corresponding automatic decryption of the encrypted data using a data structure marking the encrypted data.

Therefore, the present invention is different from Waldspurger in structures: differentiating the disk space into a VSD drive for security-sensitive files and a disk drive for a general files. Also, the present invention is different from Waldspurger in associated functions: the unauthorized application module cannot do anything about the VSD drive, and even the authorized application module cannot write out to the disk drive, by which all the security-sensitive files can be kept securely only in the VSD drive.

Waldspurger does not anticipate the features in structures and associated functions of Claim 1 of the present invention. Applicant respectfully requests withdrawal of the rejections to Claim 1.

Amended Claim 4 (*emphasis added*)

. An access control method, which is performed by an access control system having a hard disk, a disk drive, a file system module, an application module, a VSD image file module, a VSD drive, an encrypting and decrypting module, a VSD file system module, and a control access module including an extended system service table and an extended service table, wherein the VSD image file module occupies a certain space of the hard disk in a file form and the VSD drive for processing security-sensitive files is located within the VSD image file module, the access control method comprising the steps of:

(a) authorizing the application module;

(b) the application module calling a function from an operating system to access a corresponding file;

(c) the operating system providing the function to the extended service table;

(d) changing the function into an arbitrarily designated function to prevent the operation of the function in the extended service table;

(e) determining whether an access space of the file is the disk drive or the VSD drive in the extended service table;

(f) returning the arbitrarily designated function to the original function whose operation is possible, and providing the original file to the extended system service table if it is determined that the access space is the disk drive at step (e);

(g) determining whether the application module has been authorized if it is determined that the access space is the VSD drive at step (e);

(h) returning the arbitrarily designated function to the original function whose operation is possible, and providing the original function to the extended system service table if it is determined that the application module has been authorized at step (g); and

(i) stopping the operation of the corresponding function if it is determined that the application module has not been authorized at step (g).

Waldspurger Does Not Anticipate Claim 4

For similar reasons regarding to Claim 1, Waldspurger does not anticipate the structures and functions of the present invention. The cited reference does not discriminate the disk space into a VSD drive and a disk drive as in the present invention. Therefore, the associated functions get distinct from each other.

Therefore, Waldspurger does not anticipate the features in structures and associated functions of Claim 4 of the present invention. Applicant respectfully requests withdrawal of the rejections to Claim 4.

Dependent Claims

Although applicant has not addressed all the issues of the dependent claims, applicant respectfully submits that applicant does not necessarily agree with the characterization and assessments of the dependent claims made by the examiner, and applicant submits that each claim is patentable on its own merits. Claims 2-3 and 5-6 directly or indirectly depend from either independent claim 1 or 4 discussed above. Therefore, since the independent claims are not anticipated by the cited reference, Applicant respectfully requests prompt allowance of the claims.

Conclusion

In view of the amendments and remarks made above, it is respectfully submitted that claims 1-6 are in condition for allowance, and such action is respectfully solicited, if required, under *Examiner's Amendment*. If it is believed that a telephone conversation would expedite the prosecution of the present application, or clarify matters with regard to its allowance. the Examiner is invited to contact the undersigned attorney at the number listed below.

Respectfully submitted,

Date: March 11, 2009

James E. Bame

James E. Bame
Regis. No. 44521
Tel: 213-384-7200
IPLA P.A.
3580 Wilshire Blvd 17th Fl.
Los Angeles, CA 90010